IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Patent Application

Inventor(s)	Eric Henry Grosse
Case	8
Serial No.	10/805,889 Group Art Unit 2135
Filing Date	March 22, 2004
Examiner	Randal D Moran
Title	Method And Apparatus For Eliminating Dual Authentication For Enterprise Access Via Wireless LAN Services

MAIL STOP: APPEAL BRIEF – PATENTS
COMMISSIONER FOR PATENTS
P.O. Box 1450
ALEXANDRIA, VA 22313-1450

SIR:

APPEAL BRIEF UNDER 37 C.F.R. 41.37

i) Real party in interest

The real party in interest is Lucent Technologies Inc., 600 Mountain Ave., Murray Hill, NJ 07094-0636. Lucent Technologies Inc. is the owner of the entire interest in the application at issue.

ii) Related appeals and interferences

Applicants are unaware of any appeals, interferences, or judicial proceedings relating to, directly affecting, directly affected by, or having a bearing on, the Board's decision in this Appeal.

iii) Status of claims

Claims 1-7, 12-19 and 24 stand rejected under 35 U.S.C. 103(a). Claims 8-11 and 20-23 have been canceled. Applicants herein appeal the rejection of claims 1-7, 12-19 and 24.

iv) Status of amendments

There have been no amendments submitted after the mailing of the Final Office Action.

v) Summary of claimed subject matter

Over the last few years, wireless LAN (Local Area Network) services, such as those provided with use of, for example, "Wi-Fi" (the IEEE 802.11 wireless standard protocol), have become enormously popular and commonplace. From coffee houses to airport lounges, wireless LAN service "hotspots" have sprung up everywhere and wireless access to the Internet is becoming almost ubiquitous. Although a few of these wireless LAN service hotspots provide open and unrestricted network access to the Internet, being freely available to anyone who is within the necessary geographical area (typically on the order of a few hundred feet), most of these hotspots provide instead a fee-based service. In particular, for an individual user to make use of a hotspot (*i.e.*, wirelessly connect to the Internet), when the hotspot is fee-based and operated by a particular wireless LAN service provider, it is necessary to have a (previously established) account with that specific service provider. Then, any and all wireless LAN use by the given user is charged to his or her account with that service provider. Typically, establishing such an account with a wireless LAN service provider requires that the user provides credit card information (so that the given credit card can be charged for all account usage). In addition, the user will select (or be provided with) a unique user-name and a corresponding password, which is presumably unknown to others. Thus, when the user wishes to connect to the Internet through one of the given service provider's hotspots, he or she "signs on" to the wireless LAN by providing his or her user-name and corresponding password, thus authenticating that he or she is the authorized individual (who is associated with the given previously established account). From this point on, all usage of the network by the user will be advantageously charged to his or her account (*e.g.*, to the provided credit card). (See the instant specification, page 1, line 13 through page 2, line 15.)

Meanwhile, most enterprises (large corporations or other large organizations) have their own internal network (an "Intranet"), typically referred to as a "Virtual Private Network" or VPN, and many employees of these enterprises need frequent access to within the enterprise's VPN even when they are away from their home or office. In fact, when traveling on business, it is common for such enterprise employees to use such wireless LAN hotspots (*e.g.*, hotspots in airport lounges) solely to access their company's VPN, and then to access any general Internet sites (*i.e.*, those not internal to the enterprise's Intranet) from within the VPN, rather than directly through the wireless LAN service

provider. (This ensures that all of the user's access to the Internet is made from within the enterprise's "firewall," thereby providing the same level of security for the user and his or her laptop computer as if he or she were physically "inside" the enterprise's Intranet.) However, to use such wireless LAN hotspots freely, each of these employees necessarily needs an individual account with each of the different wireless LAN hotspot service operators, which not only becomes quite cumbersome, but also requires each such employee to use either a personal or corporate credit card for the charges incurred. (See the instant specification, page 2, line 16 through page 3, line 10.)

And finally, note that it is universal that a VPN will require a user to "sign on" (*i.e.*, provide a unique user-name and corresponding password to the VPN "gateway") in order to be authenticated to gain access to the VPN – otherwise, the VPN would not be "private" (*i.e.*, accessible only to authorized employees of the enterprise). Therefore, an enterprise employee who wishes to access his or her enterprise's VPN from a wireless LAN hotspot must necessarily "sign on" (be authenticated) twice – once to gain access to the wireless LAN hotspot service (and to enable the billing therefor), and once to gain access to the enterprise's VPN itself. This, especially in combination with the aforementioned fact that the user may need to use different user-names and corresponding passwords depending on the particular wireless LAN hotspot service provider at the given location, is obviously cumbersome and highly undesirable. (See the instant specification, page 3, lines 11-22.)

The instant invention provides for a method and apparatus which eliminates the need both for dual authentication and for individualized billing/payment arrangements when a user terminal (see, *e.g.*, instant Fig. 1, user 16, 17 or 18), whose user is personally associated with a given enterprise having a Virtual Private Network (VPN) (see, *e.g.*, instant Fig. 1, Enterprise-A VPN 19 or Enterprise-B VPN 20), wishes to use a wireless hotspot (or other network access) service provider (see, *e.g.*, instant Fig. 1, wireless LAN server 11), to connect to and make use of *only* its associated enterprise's VPN. More specifically, the instant invention enables the user of the user terminal to freely connect to his or her enterprise's VPN, through a corresponding gateway (see, *e.g.*, instant Fig. 1, Enterprise-A gateways 12 or 13 or Enterprise-B gateway 14), without providing any direct authentication of the user's or the user terminal's identity to the hotspot (or other network access) service provider, and without directly providing any billing or payment information whatsoever to the service provider. In particular, such an un-authenticated connection is permitted by the service provider *only* because the given enterprise and the hotspot (or other network access) service provider

have a pre-existing relationship (including, in particular, a billing arrangement) so that the cost of any access to the enterprise's VPN may be ultimately billed to the enterprise itself. (See the instant specification, page 4, line 3 through page 5, line 9.)

Specifically, independent claim 1, for example, recites a method for establishing a connection from a user terminal to a network through a network access server, the method comprising the steps of:

receiving a request from the user terminal to access the network with use of the network access server (see, *e.g.*, instant Fig. 4, block 41 or Fig. 6, block 61); and

providing limited network access to the user terminal through the network access server, without the user terminal having provided any authentication of an identity thereof to the network access server, and without the user terminal having directly provided any billing or payment information to the network access server (see, *e.g.*, instant Fig. 4, block 43 or Fig. 6, block 63),

wherein providing said limited network access comprises providing network connectivity through said network access server between said user terminal and one or more predetermined enterprise-authenticated hosts and not providing network connectivity through said network access server between said user terminal and network sites other than said one or more predetermined enterprise-authenticated hosts,

wherein said network access server is operated by a service provider, wherein said service provider has a pre-existing relationship with each of one or more known enterprises,

wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with each of said one or more known enterprises, and

wherein each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises.

Similarly, independent claim 13 recites a network access server for establishing a connection from a user terminal to a network, the network access server comprising:

means for receiving a request from the user terminal to access the network with use of the network access server; and

means for providing limited network access to the user terminal through the network access server, without the user terminal having provided any authentication of an identity thereof to the network access server, and without the user terminal having directly provided any billing or payment information to the network access server,

wherein providing said limited network access comprises providing network connectivity through said network access server between said user terminal and one or more predetermined enterprise-authenticated hosts and not providing network connectivity through said network access server between said user terminal and network sites other than said one or more predetermined enterprise-authenticated hosts,

wherein said network access server is operated by a service provider, wherein said service provider has a pre-existing relationship with each of one or more known enterprises,

wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with each of said one or more known enterprises, and

wherein each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises.

In particular, the recited "means for receiving a request from the user terminal to access the network with use of the network access server" as recited by independent claim 13 is described in the specification as comprising a network access server such as those operated by a wireless LAN hotspot service provider (see, *e.g.,* the instant specification, page 7, lines 4-12 and instant Fig. 1, wireless LAN server 11), or such a server connected by wire to, for example, a conference room or a hotel room that supplies guest network access (see, *e.g.,* the instant specification, page 5, line 20 through page 6, line 2), and adapted or programmed to perform the function as shown, for example, in instant Fig. 4, block 41 or Fig. 6, block 61. Similarly, the recited "means for providing limited network access to the user terminal through the network access server" as recited by independent claim 13 is also described in the specification as comprising a network access server such as those operated by a wireless LAN hotspot service provider (see, *e.g.,* the instant specification, page 7, lines 4-12 and instant Fig. 1, wireless LAN server 11), or such a server connected by wire to, for example, a conference room or a hotel room that supplies guest network access (see, *e.g.,* the instant

specification, page 5, line 20 through page 6, line 2), but adapted or programmed to perform the function as shown, for example, in instant Fig. 4, block 43 or Fig. 6, block 63.

vi) Grounds of rejection to be reviewed on appeal

Claims 1-7, 12-19 and 24 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Juitt *et al.* [US 2003/0087629] (hereinafter, "Juitt") in view of Deshpande *et al.* [US 2002/0176579] (hereinafter "Deshpande").

vii) Argument

a) The instant Office Action does not provide a *prima facie* case of unpatentability of independent claims 1 and 13.

Neither Juitt nor Deshpande, either alone or in combination, teach or suggest all of the limitations of either independent claim 1 or 13, and, therefore, the instant Office Action fails to provide a *prima facie* case of unpatentability of these claims. In particular, neither of these references, alone or in combination, teach or suggest allowing *un-authenticated and un-paid* access by a user terminal *only to an enterprise's VPN* through a network access server operated by a service provider. Juitt, for example, only discloses (in relevant part) that a "gateway server is interposed between wireless access points and protected networks *to provide security and integration functions*, for example, authentication, access control, link privacy, link integrity, and bandwidth metering." (See, for example, Juitt, Abstract, emphasis added.) That is, the network access service (*i.e.*, "gateway server") disclosed by Juitt necessarily *requires authentication* of the user terminal, thereby teaching away from, rather than disclosing, the instant invention as claimed.

More specifically, as admitted in the instant Office Action, "Juitt does not explicitly disclose providing limited network access without the user terminal having provided any authentication of an identity thereof to the network access server, and without the user terminal having directly provided any billing or payment information to the network access server" (see, Office Action dated October 19, 2007, page 4, lines 5-8), does not explicitly disclose "network access server is operated by a service provider, wherein said service provider has a pre-existing relationship with each of one or more known enterprises" (see, Office Action dated October 19, 2007, page 4, lines 8-10), does not explicitly disclose "wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with each of said one or more known enterprises (see, Office Action dated October 19, 2007, page 4, lines 10-12), and does not explicitly disclose "wherein each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises (see, Office Action dated October 19, 2007, page 4, lines 12-15).

However, the instant Office Action goes on to allege that each of these limitations not disclosed in Juitt is disclosed in Deshpande. Applicant respectfully disagrees. First, the instant

Office Action incorrectly alleges that "Deshpande discloses providing limited network access without the user terminal having provided any authentication of an identity thereof to the network access server . . . and without the user terminal having directly provided any billing or payment information to the network access server," citing Deshpande, paragraph [0025] lines 20-24. (See Office Action dated October 19, 2007, page 4, last 5 lines.) However, Applicant submits that this mischaracterizes the actual teaching of the reference, when taken in its entirety and compared against the instant claims. First of all, note that the instant independent claims explicitly recite that "providing said limited network access comprises providing network connectivity through said network access server between said user terminal and one or more predetermined enterprise-authenticated hosts and not providing network connectivity through said network access server between said user terminal and network sites other than said one or more predetermined enterprise-authenticated hosts." Thus, the (previously recited) limitation of the instant claims that "providing limited network access to the user terminal through the network access server, without the user terminal having provided any authentication of an identity thereof to the network access server, and without the user terminal having directly provided any billing or payment information to the network access server" must be read as "providing network connectivity through said network access server between said user terminal and one or more predetermined enterprise-authenticated hosts and not providing network connectivity through said network access server between said user terminal and network sites other than said one or more predetermined enterprise-authenticated hosts," "without the user terminal having provided any authentication of an identity thereof to the network access server, and without the user terminal having directly provided any billing or payment information to the network access server." But this is not what Deshpande paragraph [0025] discloses at all.

Rather, Deshpande paragraph [0025] discloses that if a device [mobile device 40 of Fig. 3 thereof] "is configured to register for services supplied through the access point (e.g., the device is authorized to access the services whether by the user or manufacturer of the device pre-configuring the device . . .), the device and the access point . . . establish a connection wherein the device and *user is authorized via the authentication server*(s) 50 *for access to the hotspot service provider's services.*" (See, Deshpande, paragraph [0025], lines 1-12, emphasis added.) Paragraph [0025] of Deshpande then goes on to explain that "a user/device *is required to provide* identification information such as a user name to determine whether and what types of service may be provided

and *authentication information such as a password* to confirm proper usage of the services." (See, Deshpande, paragraph [0025], lines 12-16, emphasis added.) Finally, paragraph [0025] of Deshpande continues with the language cited in the Office Action dated October 19, 2007, stating that "certain users/devices may be able to connect with and request or *accept services* from the hotspot service provider network without identification and/or authentication *such as no-charge Internet access or location-based services supported by advertisements*." (See, Deshpande, paragraph [0025], lines 20-24, emphasis added.)

That is, to the extent that Deshpande does, in fact, disclose "providing limited network access without the user terminal having provided any authentication of an identity thereof to the network access server . . . and without the user terminal having directly provided any billing or payment information to the network access server," it only provides such access to "free" hotspot service provider services. Applicants obviously do not reject the notion that free Internet access may be provided by hotspot service providers. As described in the instant specification (and as explained above), there are some wireless LAN service hotspots which provide open and unrestricted network access to the Internet, being freely available to anyone who is within the necessary geographical area. However, by reading both the instant claims and the cited paragraph of Deshpande *in their entireties*, it becomes clear that Deshpande paragraph [0025] does *not* teach or suggest "providing *limited network access* without the user terminal having provided any authentication of an identity thereof to the network access server . . . and without the user terminal having directly provided any billing or payment information to the network access server," in the manner required by the instant claims (emphasis added). In particular, it is clear that Deshpande paragraph [0025] does *not* teach or suggest "*providing* network *connectivity* through said network access server *between* said *user* terminal *and* one or more *predetermined enterprise-authenticated hosts* and *not providing* network *connectivity* through said network access server *between* said *user* terminal *and network sites other than* said one or more *predetermined enterprise-authenticated hosts*" "without the user terminal having provided any authentication of an identity thereof to the network access server, and without the user terminal having directly provided any billing or payment information to the network access server," as is specifically required by the instant claims (emphasis added).

Next, the instant Office Action incorrectly alleges that Deshpande discloses that "said service provider has a pre-existing relationship with each of one or more known enterprises . . . and wherein

each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises," citing Deshpande paragraph [0028]. (See Office Action dated October 19, 2007, page 5, lines 1-2 and 5-8.) Again, when both the instant claims and the cited portion of Deshpande are read in their entirety, it is clear that this allegation is also incorrect. Specifically, noting once again that the instant independent claims explicitly recite that "providing said limited network access comprises providing network connectivity through said network access server between said user terminal and one or more predetermined enterprise-authenticated hosts and not providing network connectivity through said network access server between said user terminal and network sites other than said one or more predetermined enterprise-authenticated hosts," it is necessary to read the limitation that "each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises" as "each of said pre-existing relationships comprises an agreement that" "providing network connectivity through said network access server between said user terminal and one or more predetermined enterprise-authenticated hosts and not providing network connectivity through said network access server between said user terminal and network sites other than said one or more predetermined enterprise-authenticated hosts" "incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises." But again, Deshpande discloses no such thing.

Rather, Deshpande discloses a "business or private mode" in which (a) "a business entity is billed for user/device usage of services from a hotspot service provider network" based on pre-existing "business arrangements" (see, Deshpande paragraph [0028], lines 3-6), and in which (b) "high encryption is used to essentially create a virtual private network (VPN) and that would be most useful to business or individual users/devices requiring high security (e.g., accessing a corporate LAN)" (see, Deshpande paragraph [0026], lines 17-21). More specifically, paragraph [0028] of Deshpande goes on to explain that "[t]his type of mode will be useful to business employees that need access to a hotspot service provider's services for a business purpose without having to establish an individual subscription with that hotspot service provider." (See, Deshpande paragraph [0028], lines 12-15.) This paragraph does not teach or suggest that *limited network access* incurs a charge billed by said service provider to a known enterprise – rather, it teaches that a business

employee (of a known enterprise) may access the hotspot as if he or she had an individual subscription thereto (*i.e.*, having *full access* – not limited access – thereto). Moreover, the cited paragraph does not teach or suggest that such access can occur *without authentication*, as is required by the instant claims – rather, when read in combination with paragraph [0026] of Deshpande, as cited above and which precedes paragraph [0028] thereof, it is abundantly clear that such "business or private mode" access not only *requires* authentication, but employs "high encryption . . . to essentially create a virtual private network (VPN) and that would be most useful to business or individual users/devices requiring high security (e.g., accessing a corporate LAN)."

And finally, even assuming *arguendo* that the individual references were to disclose the elements that are alleged in the Office Action dated October 19, 2007, the Office Action further alleges that "it would have been obvious . . . to modify the teachings of Juitt by not requiring any information prior to offering limited access to the network, a service provider having a pre-existing relationship with the enterprise, and a billing service for billing the enterprise as taught by Deshpande," because "[t]his type of mode will be useful to business employees that need access to a hotspot service provider's services for a business purpose with out having to establish an individual subscription with the hotspot service provider," citing Deshpande paragraph [0028], lines 12-15. (See, Office Action dated October 19, 2007, page 5, lines 9-16.) Applicant submits that there is no adequate justification provided in the Office Action for making such a combination – rather, the combination as made in the Office Action is clearly no more than impermissible hindsight. In other words, the Examiner is simply repeating the essence of the instant invention as if that by itself were a motivation to combine the two references. Of course, as pointed out above, these references do not show the individual limitations of the instant claims, but even assuming *arguendo* that they did, one of ordinary skill in the art would not have any basis for combining them in the manner the Examiner suggests at the time the invention was made. Although it is no longer necessary for the Examiner to provide an explicit showing in the cited references themselves of a teaching, suggestion or motivation to combine, it is nonetheless still required that an articulated reasoning with a rational underpinning for combining the elements (allegedly) taught by the references in the specific way that the claimed new invention does. This has not been done in the instant Office Action.

Thus, neither Deshpande alone, nor the combination of Juitt and Deshpande, teach or suggest allowing un-authorized (and un-paid) access by a user terminal *only* to a VPN gateway (*i.e.*, an

enterprise-authenticated host) of an enterprise's VPN through a network access server operated by a service provider. Moreover, as pointed out above, Juitt teaches away from the instant invention, thus making any such attempted combination of Juitt and Deshpande inappropriate.

(b) The instant Office Action does not provide a *prima facie* case of unpatentability of dependent claims 2-7, 12, 14-19 and 24.

For at least the above reasons, Applicants respectfully submit that the rejections of each of independent claims 1 and 13 over the cited references are improper, in that a *prima facie* case of obviousness has not been established with respect to each of these independent claims. And since each of claims 2-7, 12, 14-19 and 24 depend from one of these independent claims, the rejections of each of these claims over the same references are improper for at least the same reasons.

(c) Conclusion to the arguments

For at least the above reasons, Applicants respectfully submit that the outstanding rejections of each of claims 1-7, 12-19 and 24 are improper, and respectfully request that the Board reverse each of these rejections.

Respectfully,

Eric Henry Grosse

By _____
Kenneth M. Brown, Attorney
Reg. No. 37590
908 – 582 – 5998

Date: 3/18/08

Lucent Technologies Inc.
Docket Administrator, Rm. 2F-192
600 Mountain Avenue,
Murray Hill, New Jersey 07974-0636

viii) Claims appendix

1. A method for establishing a connection from a user terminal to a network through a network access server, the method comprising the steps of:

receiving a request from the user terminal to access the network with use of the network access server; and

providing limited network access to the user terminal through the network access server, without the user terminal having provided any authentication of an identity thereof to the network access server, and without the user terminal having directly provided any billing or payment information to the network access server,

wherein providing said limited network access comprises providing network connectivity through said network access server between said user terminal and one or more predetermined enterprise-authenticated hosts and not providing network connectivity through said network access server between said user terminal and network sites other than said one or more predetermined enterprise-authenticated hosts,

wherein said network access server is operated by a service provider, wherein said service provider has a pre-existing relationship with each of one or more known enterprises,

wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with each of said one or more known enterprises, and

wherein each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises.

2. The method of claim 1 wherein the user terminal comprises a wireless device and the network access server comprises a wireless LAN hotspot server.

3. The method of claim 2 wherein the wireless device and the wireless LAN hotspot server communicate with use of an IEEE 802.11 standard protocol.

4. The method of claim 1 wherein said request from the user terminal comprises an

identification of a given enterprise, and wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with said given enterprise.

5. The method of claim 4 wherein said user terminal has been pre-configured to automatically provide said identification of the given enterprise.

6. The method of claim 4 wherein said request from the user terminal further comprises a fixed password, said fixed password uniquely associated with said given enterprise.

7. The method of claim 6 wherein said user terminal has been pre-configured to automatically provide said identification of the given enterprise and said fixed password.

8-11. Canceled.

12. The method of claim 1 wherein said step of providing said limited network access comprises the steps of:

comparing a first IP address pair to a set of previously stored IP address pairs, the first IP address pair comprising an IP address of said user terminal and an IP address of an intended destination to which access has been requested by said user terminal, and each IP address pair in the set of previously stored IP address pairs comprising the IP address of a user terminal connected to said network access server and an IP address of one of said one or more enterprise-authenticated hosts; and

providing network connectivity between said user terminal and said intended destination if and only if said first IP address pair matches one of said IP address pairs in said set of previously stored IP address pairs.

13. A network access server for establishing a connection from a user terminal to a network, the network access server comprising:

means for receiving a request from the user terminal to access the network with use of the network access server; and

means for providing limited network access to the user terminal through the network access server, without the user terminal having provided any authentication of an identity thereof to the network access server, and without the user terminal having directly provided any billing or payment information to the network access server,

wherein providing said limited network access comprises providing network connectivity through said network access server between said user terminal and one or more predetermined enterprise-authenticated hosts and not providing network connectivity through said network access server between said user terminal and network sites other than said one or more predetermined enterprise-authenticated hosts,

wherein said network access server is operated by a service provider, wherein said service provider has a pre-existing relationship with each of one or more known enterprises,

wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with each of said one or more known enterprises, and

wherein each of said pre-existing relationships comprises an agreement that said limited network access provided to said user terminal incurs a charge billed by said service provider to a corresponding one of said one or more known enterprises.

14. The network access server of claim 13 wherein the user terminal comprises a wireless device and the network access server comprises a wireless LAN hotspot server.

15. The network access server of claim 14 wherein the wireless device and the wireless LAN hotspot server communicate with use of an IEEE 802.11 standard protocol.

16. The network access server of claim 13 wherein said request from the user terminal comprises an identification of a given enterprise, and wherein said one or more enterprise-authenticated hosts consists of one or more VPN gateways associated with said given enterprise.

17. The network access server of claim 16 wherein said user terminal has been pre-configured to automatically provide said identification of the given enterprise.

18. The network access server of claim 16 wherein said request from the user terminal further comprises a fixed password, said fixed password uniquely associated with said given enterprise.

19. The network access server of claim 18 wherein said user terminal has been pre-configured to automatically provide said identification of the given enterprise and said fixed password.

20-23. Canceled.

24. The network access server of claim 13 wherein said step of providing said limited network access comprises the steps of:

comparing a first IP address pair to a set of previously stored IP address pairs, the first IP address pair comprising an IP address of said user terminal and an IP address of an intended destination to which access has been requested by said user terminal, and each IP address pair in the set of previously stored IP address pairs comprising the IP address of a user terminal connected to said network access server and an IP address of one of said one or more enterprise-authenticated hosts; and

providing network connectivity between said user terminal and said intended destination if and only if said first IP address pair matches one of said IP address pairs in said set of previously stored IP address pairs.

ix) Evidence appendix

None.

x) Related proceedings appendix

None.